GetFullPathName

Carefully manage buffer sizes

Sean Barnum, Cigital, Inc. [vita[1]]

Copyright © 2007 Cigital, Inc.

2007-03-23

Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 4174 bytes

<table>
<tr><td><b>Attack Category</b></td><td>• Path spoofing or confusion problem</td></tr>
<tr><td><b>Vulnerability Category</b></td><td>• Buffer Overflow
• Indeterminate File/Path</td></tr>
<tr><td><b>Software Context</b></td><td>• File Path Management</td></tr>
<tr><td><b>Location</b></td><td>• winbase.h</td></tr>
<tr><td><b>Description</b></td><td>The Windows GetFullPathName() must be checked to verify that the result fits in the buffer or unexpected behavior may occur.
GetFullPathName merges the name of the current drive and directory with a specified file name to determine the full path and file name of the specified file. If the result does not fit into the return buffer, the return value is the size of the buffer that would be required to hold the path including the terminating null. It is important to check this return value, as if it is larger than the buffer size, then the buffer will not contain the complete path.</td></tr>
<tr><td><b>APIs</b></td><td><table>
<tr><th>Function Name</th><th>Comments</th></tr>
<tr><td>GetFullPathName</td><td></td></tr>
<tr><td>GetFullPathNameA</td><td></td></tr>
<tr><td>GetFullPathNameW</td><td></td></tr>
</table></td></tr>
<tr><td><b>Method of Attack</b></td><td>No attack. Reliability problem.</td></tr>
<tr><td><b>Exception Criteria</b></td><td></td></tr>
<tr><td><b>Solutions</b></td><td><table>
<tr><th>Solution Applicability</th><th>Solution Description</th><th>Solution Efficacy</th></tr>
<tr><td>Whenver GetFullPathName is used.</td><td>If the return value is larger than the buffer size, you should call the function again with a buffer that is at least as long as</td><td>Effective.</td></tr>
</table></td></tr>
</table>

[1] http://buildsecurityin.us-cert.gov/bsi/about_us/authors/35-BSI.html (Barnum, Sean)

	the indicated return value.
Signature Details	DWORD GetFullPathName(LPCTSTR lpFileName, DWORD nBufferLength, LPTSTR lpBuffer, LPTSTR* lpFilePart);

Examples of Incorrect Code	`LPCTSTR lpFileName = "SomeFile";`
	`DWORD nBufferLength = 40;`
	`LPTSTR lpBuffer = (LPTSTR)malloc(nBufferLength * sizeof(TCHAR));`
	`LPTSTR filePart;`
	`DWORD pathSize = GetFullPathName(lpFileName , nBufferLength, lpBuffer, &filePart);`
	`/* Using lpBuffer without further checks could cause trouble. */`

Examples of Corrected Code	`LPCTSTR lpFileName = "SomeFile";`
	`DWORD nBufferLength = 40;`
	`LPTSTR lpBuffer = (LPTSTR)malloc(nBufferLength * sizeof(TCHAR));`
	`LPTSTR filePart;`
	`DWORD pathSize = GetFullPathName(lpFileName , nBufferLength, lpBuffer, &filePart);`
	`if (pathSize > nBufferLength) {`
	`delete lpBuffer;`
	`nBufferLength = pathSize;`
	`lpBuffer = (LPTSTR)malloc(nBufferLength * sizeof(TCHAR));`
	`GetFullPathName(lpFileName , nBufferLength, lpBuffer, &filePart);`
	`}`
	`/* Using lpBuffer now should be safe. */`

Source Reference	http://www.freelists.org/archives/windows_errors/06-2003/msg00007.html
Recommended Resource	MSDN reference page for GetFullPathName[3]
Discriminant Set	**Operating System**: Windows **Languages**: C C++

Cigital, Inc. Copyright

Copyright © Cigital, Inc. 2005-2007. Cigital retains copyrights to this material.

Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and “No Warranty” statements are included with all reproductions and derivative works.

For information regarding external or commercial use of copyrighted materials owned by Cigital, including information about “Fair Use,” contact Cigital at copyright@cigital.com[1].

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

[1] mailto:copyright@cigital.com